Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Nämnden för inköp och upphandling

2022-12-22

Innehåll

1 Dataskydd i kommunal verksamhet

Att få ta del av och hantera andra människors personliga uppgifter på ett sådant sätt som kommunala förvaltningar och bolag gör innebär att förvalta ett stort förtroende. Dataskyddsförordningen (GDPR) har tillkommit för att särskilt skydda människors rätt till integritet, och för att värna var och ens rätt att få ha kontroll över vad som sker med uppgifter om ens person. Att förvaltningar och bolag hanterar personuppgifter i enlighet med gällande lag bör vara en självklarhet i syfte att visa omsorg om det förtroende som givits den som har att hantera uppgifterna.

Arbetet med att säkerställa att personuppgifter behandlas enligt reglerna i GDPR behöver genomsyra arbetet inom de kommunala verksamheterna på alla olika plan. Det gäller allt från rutiner och processer för det dagliga arbetet, till arbetet med innovations- och digitaliseringslösningar för framtidens arbetssätt på förvaltningar och bolag inom Göteborgs Stad. I det framåtsyftande arbetet är GDPR ett viktigt redskap för att kunna säkerställa en digitalisering som håller över tid.

1.1 Göteborgs Stads dataskyddsombud

Dataskyddsenheten på Intraservice är Göteborgs Stads dataskyddsombud. Vad som är dataskyddsombudets uppgifter framgår direkt av lagstiftningen i GDPR.[1] Dataskyddsombudets viktigaste uppgift är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. Detta sker bland annat genom att samla in information om hur personuppgifter behandlas och genom att kontrollera hur bestämmelser och interna styrdokument som styr dataskyddsarbetet efterlevs.

Dataskyddsombudet har också till uppgift att ge råd och information till förvaltningar och bolag i dataskyddsfrågor. Detta sker genom att dataskyddsombudet är behjälplig när frågor rörande behandlingen av personuppgifter uppkommer hos verksamheterna. Dataskyddsombudet erbjuder också regelbundet utbildningar för stadens medarbetare. Rådgivning ges även till förvaltningar och bolag när dessa genomför konsekvensbedömningar, vilket är en skyldighet som följer av GDPR. Efter att ha identifierat ett särskilt behov av stöd i arbetet med konsekvensbedömningar, har dataskyddsenheten under 2022 tagit fram mallar och mallstöd för det arbetet.

Det är nämnd/styrelse som har det yttersta ansvaret för att verksamheterna följer dataskyddslagstiftningen och dataskyddsombudet ska enligt lag rapportera om detta till högsta förvaltningsnivå.[2] Dataskyddsombudet har inte mandat att fatta beslut åt verksamheterna. Det är i stället genom råd och rekommendationer som dataskyddsombudet bistår verksamheterna med underlag för att dessa själva ska kunna fatta väl underbyggda beslut.

[1] Artikel 39 i GDPR
[2] Artikel 38.3 i GDPR

2 Granskning av dataskyddsarbetet 2022

2.1 Dataskyddsombudets kontrollfunktion

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras i artikel 39 i GDPR. I Göteborgs Stad innebär en del av denna övervakning att dataskyddsombudet genomför kontroller av dataskyddsarbetet inom den personuppgiftsansvariges organisation.

Enligt dataskyddsregelverket ska dataskyddsombudet arbeta utifrån en riskbaserad metod som utgår från risker för de registrerades fri- och rättigheter. Genom att utgå från en sådan metod minskas risken för negativa konsekvenser även för verksamheten själv. Sådana konsekvenser kan omfatta bland annat skadestånd, sanktionsavgifter, försämrat varumärke eller minskad tillit för verksamheten.

För dataskyddsombudet är kontrollarbetet ett sätt att få en bild av vilka risker och/eller brister som eventuellt föreligger inom en verksamhet. Genom kontroller kan dataskyddsombudet kartlägga verksamhetens dataskyddsarbete, och därigenom hjälpa verksamheten att få en nulägesbild av hur de faktiskt ligger till i sitt dataskyddsarbete. Denna kartläggning kan sedan användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Kontrollarbetets syfte är inte främst att peka ut brister utan ska ses som en vägledning för verksamheten och ett verktyg för att identifiera relevanta prioriteringar. Det är sedan upp till varje verksamhet att besluta om hur det interna dataskyddsarbetet ska utformas utifrån verksamhetens förutsättningar för att på bästa sätt kunna hantera identifierade risker. I det arbetet är dataskyddsombudet behjälplig med rådgivning utifrån verksamhetens behov och de risker som identifierats.

2.2 Fördjupad kontroll

2.2.1 Kontroll av behörighetsstyrning 2022

Under 2022 har dataskyddsombudet genomfört en fördjupad kontroll där verksamhetens arbete med behörighetsstyrning i IT-systemet Tendsign har granskats. Syftet med kontrollen är att granska om dataskyddsombudet ser risker i verksamhetens arbete med behörighetsstyrning utifrån kraven i artikel 32 i GDPR.

Dataskyddsombudet har i rapporten avseende den fördjupade kontrollen haft vissa anmärkningar och därför lämnat ett antal rekommendationer till verksamheten. Förvaltningen rekommenderas att:

- Ta fram skriftliga rutiner för hur hantering av åtkomstkontroll/kontroll av loggar får gå till för att inte utsätta de anställda för övervakning/integritetsrisker.

- Uppdatera rutinen för behörighetshantering med att behörigheter även ska ses över även vid byte av tjänst.
- Eftersom förvaltningen har en pågående upphandling för ett system som ska ersätta Tendsign är det viktigt att man kravställer utifrån korrekt behörighetsstyrning. Förvaltningen rekommenderas också att säkerställa så personuppgiftsbiträdesavtal och instruktioner reglerar biträdets åtkomst till personuppgifter i systemet.

2.3 Årlig kontroll av dataskyddsarbetet

Verksamhetens interna dataskyddsarbete följs årligen upp genom en enkät. Enkäten består av tolv punkter (”fasta kontrollpunkter”) där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Enkäten är avsedd att spänna över de viktigaste delarna inom dataskyddsarbetet för att på så sätt fånga in en större bredd av frågor. Metoden syftar till att få till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

2.3.1 Metod och risknivåer

I arbetet används en modell som består av fyra kategorier, vilka representerar fyra olika risknivåer. Verksamheten får utifrån sina svar ett värde som visar vilken risknivå verksamheten befinner sig på inom respektive kontrollpunkt. Genom att arbeta med risknivåer möjliggörs ett riskbaserat arbetssätt för både verksamhet och dataskyddsombud, då resultaten ger en bild av vad verksamheten behöver prioritera i dataskyddsarbetet framåt.[3]

Beskrivning av risknivåer

Risknivåer	Färgkod
Nivå 1. Höga risker identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten.	
Nivå 2. Risker identifierade som bedöms vara omfattande och/eller kräver omgående åtgärder.	
Nivå 3. Risker identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.	
Nivå 4. Inga direkta risker av betydelse identifierade. Indikerar att verksamheten har ett systematiskt dataskyddsarbete.	

[3] I arbetet med enkäten har dataskyddsenheten utgått från Myndigheten för samhällsskydd och beredskaps (MSB) uppföljningsstruktur för den offentliga förvaltningens systematiska informationssäkerhetsarbete.

2.4 Inköp och upphandlings dataskyddsarbete 2022

I detta avsnitt anges vilken risknivå verksamheten befinner sig inom för respektive kontrollpunkt, baserat på verksamhetens svar på de fasta kontrollpunkterna. Under varje kontrollpunkt presenteras även dataskyddsombudets bedömning gällande verksamhetens risker utifrån de iakttagelser som dataskyddsombudet gjort under året.

2.4.1 Kontrollpunkt 1: Dataskyddsorganisation

Kontrollpunkten avser verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete, och omfattar bland annat verksamhetens dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt tillhandahållna resurser för arbetet.

Dataskyddsombudets kommentarer:

Dataskyddsombudet instämmer i förvaltningens skattning gällande den interna dataskyddsorganisationen. Det kan konstateras att för få resurser har lagts på dataskyddsarbetet vilket gör att den interna organisationen inte hinner med alla de uppgifter som behöver göras. Under året har förvaltningen periodvis varit utan dataskyddskontakt helt eller delvis vilket har påverkat arbetet på förvaltningen. Nya styrande dokument har tagits fram där det framkommer att förvaltningen alltid ska ha två dataskyddskontakter som delar på arbetet. Dataskyddsombudet ser positivt på de vidtagna åtgärderna, då förvaltningen i sin nya roll som tjänsteleverantör kommer att behöva jobba mycket med dataskyddsfrågor. Bägge dataskyddskontakterna har andra arbetsuppgifter vilket gör att det är svårt att prioritera dataskyddsfrågorna. Förvaltningen bör se över hur man kan tillföra mer resurser till dataskyddsorganisationen samt definiera vilka befattningar/roller som har mandat att fatta beslut kopplat till dataskydd. Förvaltningen uppger att det saknas definierade rapporteringsvägar, vilket gör det svårt att lyfta dataskyddsfrågor uppåt i organisationen och är något som dataskyddsombudet rekommenderar att förvaltningen vidtar åtgärder för att ändra på.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att identifiera och hantera personuppgiftincidenter.

Dataskyddsombudets kommentarer:

Dataskyddsombudet instämmer i förvaltningens bedömning avseende hantering av personuppgiftsincidenter. Dataskyddsombudet har tidigare granskat förvaltningens arbete och de rekommendationer som lämnades då har åtgärdats. Den generella kunskapen om incidenter kan höjas inom förvaltningen. Uppföljning av tidigare inträffade incidenter är ett sätt för förvaltningen att se mönster och kunna vidta åtgärder innan incidenter sker. Under året har ingen incident rapporterats eller dokumenterats, vilket dataskyddsombudet bedömer som osannolikt utifrån verksamheten och antalet personuppgifter som behandlas.

2.4.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Kontrollpunkten avser verksamhetens dokumentation av biträdesavtal och andra överenskommelser gällande dataskydd, och förutsätter att verksamheten har identifierat samt registrerat personuppgiftsbiträden i personuppgiftsregistret. Även verksamhetens rutiner för uppdatering och uppföljning av tecknade biträdesavtal innefattas.

Dataskyddsombudets kommentarer:

Dataskyddsombudet instämmer i förvaltningens bedömning och anser att det finns en del kvar att göra när det kommer till hanteringen av biträden och biträdesavtal. Kontrollpunkten var planerad som fördjupad kontroll 2021 men på grund av att inga svar inkom ifrån förvaltningen kvarstår det som en granskning som behöver göras.

Dataskyddsombuden ser framför allt en stor risk när det kommer till förvaltningens kompetens att bedöma hela kedjan av underbiträden vid anlitandet av personuppgiftsbiträde. Det är också viktigt att förvaltningen tar fram en rutin för att kunna genomföra efterlevnadskontroller för redan anlitade biträden för att säkerställa att de följer vad som avtalats.

2.4.4 Kontrollpunkt 4: Personuppgiftsregister

Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även verksamhetens arbete med, och rutin för, att säkerställa ett uppdaterat och heltäckande personuppgiftsregister innefattas.

Dataskyddsombudets kommentarer:

Personuppgiftsregistret var en del av den fördjupade kontrollen 2021 och de rekommendationer som dataskyddsombudet lämnade då kvarstår eftersom förvaltningen inte vidtagit några åtgärder. Förvaltningens skattning i år visar på att förvaltningen har en bättre förståelse för hur det faktiska arbetet ser ut och hur arbetet med registret fungerar. Eftersom ingen översyn gjorts sen 2019 behöver mycket arbete med registret göras och dataskyddsombudet bedömer att höga risker föreligger som kräver åtgärder. Framför allt behöver gamla behandlingar ses över och en rutin för hur nya behandlingar förs in behöver tas fram. Ett utpekat ansvar för registret behövs också. Dataskyddsombudet bedömer att det faktiska arbetet är beroende av att förvaltningen tillsätter ytterligare resurser till dataskyddsarbetet.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Dataskyddsombudet instämmer i förvaltningens skattning och är av uppfattningen att förvaltningen saknar en övergripande strategi för dataskydd. Denna uppfattning grundar sig på det faktum att förvaltningen saknar en större och resursstark intern dataskyddsorganisation som sköter planering, uppföljning och kontinuerligt arbete med dataskyddsfrågor i förvaltningen. Det finns inget aktivt och medvetet riskbaserat arbetssätt eftersom det inte finns ett förvaltningsövergripande arbetssätt kopplat till dataskyddsfrågor. Förvaltningen rekommenderas att ta fram en informationssäkerhetspolicy för behandling av personuppgifter, säkerställa att styrande dokument som reglerar personuppgiftsbehandlingar hålls uppdaterade samt se över informationstillgångar och värdera dem utifrån konfidentialitet/riktighet/tillgänglighet enligt stadens styrande dokument.

Vidare vill dataskyddsombudet särskilt lyfta riskerna med avsaknad av rutiner för att följa GDPR vid anordnande av event. Förvaltningen uppger att de regelbundet anordnar olika typer av event där personuppgifter behandlas, till exempel deltagarlistor och matallergier. Dataskyddsombudet rekommenderar att rutiner tas fram för att minska risken för att de registrerades personuppgifter behandlas felaktigt vid möten, evenemang, föreläsningar o.s.v. Slutligen bör förvaltningen lyfta in dataskyddsperspektivet i andra interna kontroller/efterlevnadskontroller för att säkerställa att förvaltningen följer GDPR.

2.4.6 Kontrollpunkt 6: Utbildning

Kontrollpunkten avser verksamhetens arbete med att utbilda och upprätthålla kunskapsnivån i dataskyddsfrågor hos anställda.

Dataskyddsombudets kommentarer:

Dataskyddsombudet instämmer i förvaltningens bedömning. Förvaltningen har tidigare vidtagit åtgärder för att tillhandahålla utbildningsinsatser för medarbetarna men dataskyddsombudets uppfattning är att det saknats på senare år. Dataskyddsombudet instämmer i att den generella kunskapen inom förvaltningen bör höjas och att förvaltningen behöver se över vilka allmänna och riktade utbildningsinsatser som kan vidtas. Förvaltningen rekommenderas kartlägga behov och säkerställa att man följer upp och bibehåller kunskapsnivån i verksamheten.

Dataskyddsombudet vill särskilt rekommendera en riktad insats mot de som arbetar med kravställningar och upphandlingar, då dataskyddskompetens saknas i organisationen.

2.4.7 Kontrollpunkt 7: Integritetspolicy

Kontrollpunkten avser verksamhetens utformning samt tillhandahållande av dess integritetspolicy till registrerade (både internt och externt). Även verksamhetens rutin för att upprätthålla en aktuell integritetspolicy omfattas.

Dataskyddsombudets kommentarer:

Förvaltningens integritetspolicy är nyligen reviderad av dataskyddskontakten och enligt information ska den regelbundet ses över. Dataskyddsombudet har inte granskat förvaltningens nya integritetspolicy, men har ingen anledning att ifrågasätta förvaltningens bedömning. Dataskyddskontakten har informerat dataskyddsombudet om att förvaltningen har identifierat två prioriterade områden där informationsfrågan är viktig. Det rör sig dels om information till anställda både vid anställning och vid t.ex. fotografering, presentationer, digitala möten och utbildningar, dels om att säkerställa att förvaltningens digitala kanaler uppdateras med aktuell information. Dataskyddsombudet instämmer i förvaltningens bedömning och rekommenderar förvaltningen att fokusera på de två identifierade punkterna.

2.4.8 Kontrollpunkt 8: E-post och dokumenthantering

Kontrollpunkten avser verksamhetens rutiner för e-post och dokumenthantering. I detta är en aktuell och fastställd dokumenthanteringsplan med gallringsbeslut en förutsättning för att verksamheten ska kunna säkra följsamhet gentemot dataskyddsförordningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Dataskyddsombudets kommentarer:

Förvaltningen har uppgett övervägande låga svar på kontrollpunkten vilket tyder på att höga risker föreligger som kräver åtgärder. Dataskyddsombudet instämmer i bedömningen. En uppdaterad dokumenthanteringsplan med gallringsrutiner är en förutsättning för att förvaltningen ska kunna säkerställa principen om lagringsminimering enligt GPDR. Förvaltningen rekommenderas också se över hur medarbetarna informeras om dokumenthantering och gallring, då det också säkerställer medarbetarnas möjlighet att själva följa GDPR. Det är också en stor risk att förvaltningen inte har någon uppfattning om hur stor andel av verksamhetens personuppgiftsbehandlingar som har informationsklassificerats utifrån stadens riktlinje om informationssäkerhet. Förvaltningen rekommenderas att åtgärda detta.

2.4.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras, samt rutiner kopplat till detta.

Dataskyddsombudets kommentarer:

Förvaltningen uppger som komplement till skattningen att en ny rutin tagits fram som ska styra arbetet med konsekvensbedömningar. Dataskyddsombudet har inte granskat rutinen, men ser positivt på de vidtagna åtgärderna. Dataskyddsombudet anser dock att de är viktigt att den nya rutinen implementeras och följs i förvaltningen för att de ska ha någon effekt. Det finns inga tidigare genomförda tröskelanalyser eller konsekvensbedömningar på förvaltningen, trots att det högst troligt finns behandlingar som skulle kräva det. Dataskyddsombudet rekommenderar förvaltningen att se över behandlingar som redan är påbörjade och identifiera vilka som innebär höga risker för de registrerades fri- och rättigheter och därefter genomföra konsekvensbedömningar vid behov.

2.4.10 Kontrollpunkt 10: IT-projekt och upphandling

Kontrollpunkten avser verksamhetens organisation och rutiner för hantering av dataskyddsfrågor inom IT-projekt och upphandling. I detta ingår till exempel hur verksamheten integrerar dataskyddsfrågor i arbetet med upphandling av nya, samt utvecklingen av, befintliga system och tjänster.

Dataskyddsombudets kommentarer:

Förvaltningen har skattat sig själva lågt på kontrollpunkten och dataskyddsombudet instämmer i den bedömningen. Det är stor risk att dataskyddsperspektivet missas vid upphandling, och när det sedan kommit in långt senare kan det orsaka problem

i form av att tjänster som upphandlats inte är förenliga med GDPR. Dataskyddsombuden upplever också att det saknas kunskap hos medarbetarna i vilka frågor de bör lyfta in i upphandlingar. Dataskyddsombuden rekommenderar att förvaltningen tar fram ett övergripande arbetssätt för att underlätta för projekten och säkerställa att dataskyddsperspektivet omhändertas tidigt i processerna. Det bör också vara tydligt att dataskyddsombuden ska involveras, men kunskapen om vad dataskyddsombudet gör och dess roll bör förtydligas. Förvaltningens låga skattning visar på att det föreligger stora risker på den här kontrollpunkten vilket dataskyddsombudet instämmer i. Det är framför allt viktigt utifrån förvaltningens roll som vägledande/stöttande inom upphandling, att medarbetarna också har kompetens att kravställa inom dataskyddsområdet. Dataskyddsombudet har flertalet gånger blivit involverad i upphandlingar där kompetens kring dataskydd saknats. Förvaltningen rekommenderas att se över medarbetarnas kompetens och arbetssätt för att de ska kunna göra nödvändiga bedömningar av leverantörer och behandlingar, särskilt kopplat till IT-system och molntjänster.

2.4.11 Kontrollpunkt 11: IT-system och digitala verktyg

Kontrollpunkten avser verksamhetens rutiner för att säkerställa att verksamhetens personuppgiftshantering inom ramen för IT-system och digitala verktyg är förenlig med dataskyddsförordningen. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår även.

Dataskyddsombudets kommentarer:

Förvaltningens låga skattning tyder på att det föreligger höga risker och att det finns många åtgärder att vidta kopplat till IT-system och digitala verktyg. Dataskyddsombudet vill framför allt lyfta vikten av att ha rutiner för tilldelning av behörigheter och åtkomster samt uppföljning av dessa. Ett grundläggande förhållningssätt är att medarbetare bara ska behandla och komma åt sådana personuppgifter som de behöver i sin yrkesutövning.

Dataskyddsombudet bedömer att dataskyddsperspektivet ofta saknas vid införandet och användandet av kostnadsfria tjänster såsom gratisappar och sociala medier, men också vid vidareutvecklandet av redan existerande tjänster som innebär personuppgiftsbehandling. Detta har att göra med att dataskyddsperspektivet och kunskapen om dataskydd inte säkerställs hos alla i förvaltningen. Dataskyddsombudet vill också särskilt lyfta användningen av både cookies och sociala medier som något som förvaltningen bör se över omgående utifrån de risker som kan föreligga. Förvaltningen rekommenderas också ta fram en heltäckande och uppdaterad dokumentation över samtliga IT-system/digitala verktyg samt en dokumenterad överblick över förvaltningens kommunikationskanaler.

2.4.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering.

Dataskyddsombudets kommentarer:

Dataskyddsombudet ser ingen anledning att ifrågasätta förvaltningens bedömning av kontrollpunkten. Dataskyddsombudet har inte blivit involverad i några frågor gällande registrerades rättigheter under året och saknar därför inblick i hur arbetet med att säkerställa dessa fungerar på förvaltningen. Förvaltningen uppger att arbete pågår med att ta fram en rutin för hantering av registrerades rättigheter, vilket dataskyddsombudet ser som positivt. Medvetenheten gällande registrerades rättigheter är kopplat till den generella kunskapen om dataskydd och kan alltid höjas. Förvaltningen rekommenderas, att i de fall som samtycke används, ta fram en rutin för hur förvaltningen hanterar ett eventuellt tillbakadragande av samtycke. Detta eftersom det är en förutsättning för att samtycket ska vara lagligt enligt GDPR.

2.5 Särskilda iakttagelser under året

2.5.1 Tjänsteleverantör i ny styrmodell för digitalisering

Dataskyddsombudet vill särskilt lyfta frågan om förvaltningens egen roll som eventuellt personuppgiftsbiträde när den nya styrmodellen för digitalisering börjar gälla efter årsskiftet. Dataskyddsperspektivet har inte omhändertagits i projektet vilket har inneburit problem för alla tre tjänsteleverantörer i den nya styrmodellen. Dataskyddsombudet rekommenderade i förra årets årsrapport att frågan om roller och ansvar i nya styrmodellen skulle utredas innan införandet, vilket alltså inte har gjorts. Dataskyddsombudet bedömer att det innebär stora risker att utredningen inte gjorts och att förvaltningarna först två månader innan införandet började titta på frågan. Dataskyddsombudet anser att detta beror på bristande kompetens kopplat till både dataskydd och vad rollen som personuppgiftsbiträde/leverantör innebär. Riskerna med att inte ha säkerställt dataskyddsperspektivet inför införandet är att det är otydligt vem som är ansvarig för vad och hur detta ska regleras.

2.6 Sammanfattande rekommendationer

För att på ett praktiskt plan kunna identifiera vad verksamheten behöver arbeta med inom ramen för respektive kontrollpunkt behövs en noggrann genomgång av enkätresultaten. I detta rekommenderas verksamheten att samråda med dataskyddsombudet för att se hur arbetet framåt bör utformas och vilka delar som

bör prioriteras utifrån verksamhetens risker. Även för verksamheter med låga risker krävs kontinuerliga insatser för att denna risknivå ska bibehållas.

Utifrån identifierade risker rekommenderar dataskyddsombudet att förvaltningen/bolaget under 2023 prioriterar följande delar av dataskyddsarbetet:

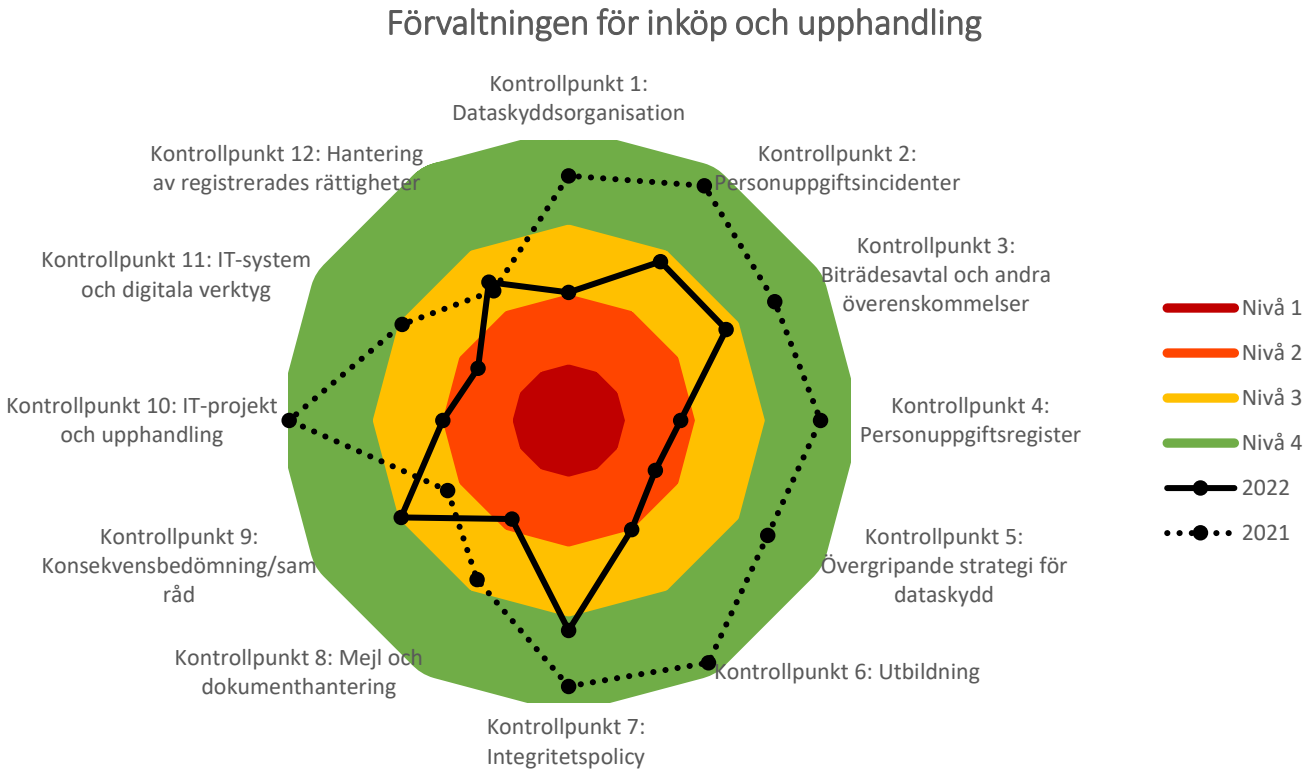
- Kontrollpunkt 10: IT-projekt och upphandling
  Utifrån förvaltningens roll i staden och det uppdrag som finns rekommenderas förvaltningen höja medarbetarnas kompetens om dataskydd för att kunna kravställa på ett sätt som är förenligt med GDPR.
- Kontrollpunkt 5: övergripande strategi för dataskydd
  Förvaltningen rekommenderas ta fram en övergripande strategi för dataskydd som utgår ifrån ett riskbaserat arbetssätt.
- Kontrollpunkt 4: personuppgiftsregister
  Förvaltningen rekommenderas se över registret och uppdatera det utifrån gällande behandlingar, ta fram rutin för hur nya behandlingar ska föras in samt vem som är ansvarig för arbetet.

3 Bilagor

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.

Bilaga 2: Fördjupad kontroll 2022 – behörighetsstyrning

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.



Bilaga 2

Fördjupad kontroll

Behörighetsstyrning Inköp- och upphandling

Bakgrund

Den fördjupade kontrollen av behörighetsstyrning syftar till att se om verksamhetens hantering av personuppgifter är säker och korrekt utifrån både tekniska och organisatoriska åtgärder. Med utgångspunkt i artikel 32.2 har kontrollen granskat verksamhetens bedömning av lämplig säkerhetsnivå med hänsyn till risker i synnerhet från bland annat obehörig åtkomst till personuppgifter. Därför har fokus legat på behörighetsstyrning och hur det används för att begränsa vilka personuppgifter som medarbetarna får ta del av.

Kontrollen har genomförts i två delar, den första som ett generellt frågeutskick och den andra som ett kompletterande frågeutskick. I kontrollen ingick verksamhetens rutiner för tilldelning av behörigheter och åtkomster i ett särskilt utvalt IT-system, uppföljning av behörigheter samt användning av logg-/åtkomstkontroller.

Iakttagelser från kontrollen

En medarbetare i en verksamhet ska enbart ha tillgång till personuppgifter som är anpassade och begränsade till det som är nödvändigt för att medarbetaren ska kunna utföra sina arbetsuppgifter. För att säkerställa detta bör verksamheten ha rutiner för tilldelning av behörighet, uppföljning av behörigheter samt hur användningen av logg-/åtkomstkontroller sker.

Behörighetsstruktur och roller i system

Kontrollen rörande inköp- och upphandlings behörighetsstyrning har haft fokus på IT-systemet TendSign. Inköp- och upphandling har ett eget avtal med systemleverantören Mercell TendSign och således även en egen uppsättning av systemet.

Endast de användare som inköp- och upphandling tilldelar behörighet har tillgång till systemet och förvaltningens upphandlingar och avtal. Systemets behörighetsstruktur är uppbyggt utifrån förvaltningens organisation med olika avdelningar och enheter.

Inköp- och upphandlings systemförvaltare/administratör ansvarar bland annat för att lägga upp nya användare i systemet inom respektive avdelning/enhet och tilldela användaren aktuella rättigheter för att skapa egna upphandlingar och avtal (*Bilaga 1*). Användaren placeras även in i en eller flera mallgrupper som ger användaren läs- eller skrivrättigheter i andra användares upphandlingar och/eller avtal i systemet.

Det finns möjlighet att lägga upp tillfälliga användare i systemet, exempelvis en tillfällig konsult som anlitas för att genomföra en upphandling för Inköp- och upphandlings räkning. Tillfälliga användare sorteras inte in i någon mallgrupp och har således endast behörighet till sina egna upphandlingar/avtal i systemet. Samtliga användare och tillfälliga användare tilldelas tillsvidarebehörighet som kan inaktiveras vid behov, exempelvis i det fall en användares anställning eller uppdrag upphör på inköp- och upphandling.

Tilldelning av behörighet utifrån bedömning

Förvaltningen har angett att systemet har två moduler – en för upphandlingsprocessen och en för avtalsprocessen. När en ny upphandling skapas i systemet ges följande mallgrupper behörighet till upphandlingen:

• "Admin”: systemförvaltare/administratör, skrivrättigheter
• “INK alla”: samtliga användare på förvaltningen, läsrättigheter
• “Projektgrupp”: samtliga eventuella projektgruppsdeltagare på förvaltningen, läsrättigheter Inköp och upphandling 2 (3)

När ett nytt avtal skapas i systemet ges följande mallgrupper behörighet till avtalet:

• "Admin": systemförvaltare/administratör, skrivrättigheter
• "INK alla": samtliga användare på förvaltningen, läsrättigheter
• "Upphandlingsassistenter": samtliga eventuella upphandlingsassistenter på förvaltningen, skrivrättigheter

Förutom vad som anges ovan kan ansvarig användare som skapat upphandlingen/avtalet även skapa egna grupper med användare eller gästanvändare och tilldela dessa skriv- eller läsrättigheter. Rättigheterna kan anges som tills vidare eller tidsatta med ett visst slutdatum.

Beslut om behörighet

Enligt rutin vid nyanställning (*Bilaga 2, punkt Skapa användarkonto i upphandlingsverktyg (för berörda)* meddelar chef systemadministratören när en ny användare ska tilldelas ett användarkonto i systemet. Härtill finns även en rutin för avslut av anställning (*Bilaga 3, punkt Avsluta användarkonto i upphandlingsverktyg*).

Uppföljning av behörighet

Den som har kvar sin anställning och roll på förvaltningen behåller de behörigheter denne behöver för att utföra sina arbetsuppgifter. Om personen byter roll eller avdelning på förvaltningen uppdateras behörigheten vid behov för att passa den nya rollen, när systemförvaltaren uppmärksammas om detta. Det finns ingen specifik rutin för uppdatering av behörighet vid byte av anställning inom organisationen utan detta är behovsstyrt.

Systemförvaltaren genomför kontroll av behörigheterna cirka 1–2 gånger per år. Kontroll genomförs för att se vilka användare och tillfälliga användare som finns registrerade på vilken avdelning/enhet i organisationsstrukturen samt vilka mallgrupper användarna är kopplade till. Eventuella justeringar genomförs vid behov. Det går inte att manuellt radera gamla användare, endast inaktivera dem. För att radera dem helt ur systemet krävs en beställning till systemleverantören.

Åtkomstkontroll/kontroll av loggar

Förvaltningen anger att respektive upphandling/avtal innehar en automatisk journal där upphandlingsprocessens händelser loggas, exempelvis över vilka användare som annonserat, öppnat eller tilldelat en upphandling samt när i tid. Majoriteten av dokumenten i systemet utgörs av elektroniska dokument, exempelvis upphandlingsdokument, avtal och interna dokument såsom tilldelningsbeslut. Dessa innehar en automatisk historik där händelser loggas med tidsstämpel där det går att se vilka användare som gjort ändringar i dokumentet.

Annan lagstiftning/bestämmelser som påverkar behörighetstilldelningen

- *19 kap. Sekretess till skydd för det allmännas ekonomiska intresse* 1 § (Affärs- och driftförhållanden), 3 § (Upphandling m.m.), 6 § (Förhandlingar) och 9 § (Rättsliga tvister)
- *31 kap. Sekretess till skydd för enskild i annan verksamhet med anknytning till näringslivet* 16 § (Enskildas ekonomiska intressen vid affärsförbindelse med myndighet)

Andra åtgärder

Då anbud omfattas av total sekretess är det tekniskt omöjligt för någon att komma åt anbud innan sista anbudsdagen har passerat. När anbuden öppnas skapas automatiskt dokumentation enligt gällande lagstiftning.

Del 1

Förvaltningen har uppgett att det går att följa upp och kontrollera loggar i systemet, men att det saknas en skriftlig rutin för detta i dagsläget. Med tanke på att det är tekniskt möjligt att följa upp händelser i systemet, rekommenderar dataskyddsombudet inköp- och upphandling att ta fram en sådan rutin.

Förvaltningen har inte identifierat att några personuppgiftsincidenter kopplat till felaktig behörighetstilldelning ägt rum. Det är positivt att förvaltningen inte har några incidenter att rapportera kopplat till hanteringen, likväl rekommenderar dataskyddsombudet att rutinen följs upp när det nya systemstödet införs för att säkerställa en likvärdig hantering.

Del 2

Förvaltningen uppger att cirka 90 personer har behörighet till systemet. Personuppgiftsbiträdet har endast behörighet att se systemet och användare, men inga ytterligare uppgifter däri. För att personuppgiftsbiträdet ska få tillgång till övriga uppgifter läggs tidsbegränsad supportbehörighet per gång, vilket framgår i det personuppgiftsbiträdesavtal som förvaltningen skickat med som bilaga (*Bilaga 1. Personuppgiftsbiträdesavtal Visma Commmerce TendSign Upphandlare*).

Förvaltningen uppger att en konsekvensbedömning inte behöver göras då man bedömt att behandlingen av personuppgifter sannolikt inte leder till en hög risk för enskilda personers fri- och rättigheter enligt artikel 35.3 eller utifrån de nio kriterier som ska beaktas enligt Artikel 29-gruppens riktlinjer om konsekvensbedömning. Vid införandet av GDPR genomfördes en riskanalys av inköp- och upphandlings personuppgiftsbehandlingar enligt *Bilaga 2*. Riskanalysen utgick från förvaltningens processer och inte per systemstöd som TendSign. Det har även gjorts en kartläggning över förvaltningens personuppgiftsbehandlingar med informationsklassning enligt *Bilaga 3*.

I TendSign behandlas främst personuppgifter såsom namn och kontaktuppgifter för användare och leverantörer som lämnat anbud eller tecknat avtal med förvaltningen. Endast i undantagsfall behandlas skyddsvärda eller känsliga personuppgifter vilket i sådana fall lämnas av anbudsgivaren i CV eller där organisationsnumret för en enskild firma är detsamma som personnummer. De risker som har identifierats kopplat till den nuvarande hanteringen av behörigheter är en mer övergripande fråga om informationssäkerhet och att säkerställa att handlingar tas omhand för arkivering eller att gallring verkställs som en del av arkivvården. Trots detta rekommenderar dataskyddsombudet inköp- och upphandling att följa upp och förtydliga hur ofta det förekommer att särskilt skyddsvärda eller känsliga personuppgifter behandlas i systemet.

Sammanfattade rekommendationer

- Förvaltningen bör ta fram skriftliga rutiner för åtkomstkontroll/kontroll av loggar i systemstödet.
- Se över om rutin behövs för uppdatering av behörighet vid byte av tjänst.
- Följ upp de krav som förvaltningen ställt kopplat till behörighetsstyrning i vilka dataskyddsombudet instämmer i.
- Eftersom förvaltningen upphandlar ett nytt system är rekommendationerna inte längre aktuella för nuvarande system, men förvaltningen rekommenderas i stället att säkerställa korrekt behörighetsstyrning i det nya systemet.

Bilagor

1. Informationsutskick fördjupad kontroll behörighetsstyrning
2. Frågeutskick del 1
3. Frågeutskick del 2

Information om fördjupad kontroll 2022

Kontrollpunkt 11: Behörighetsstyrning

För att säkerställa säkerheten och en korrekt personuppgiftshantering inom en verksamhet behöver både tekniska och organisatoriska åtgärder vidtas. Exempel på tekniska säkerhetsåtgärder är att system utformas så att endast behöriga personer kan göra sökningar och att det finns behörighetskontrollsystem. En viktig och effektiv organisatorisk åtgärd i en verksamhet är behörighetsstyrning.

I artikel 32.2 i dataskyddsförordningen ställs krav på att den personuppgiftsansvarige i samband med bedömning av lämplig säkerhetsnivå ska ta särskild hänsyn till risker i synnerhet från bland annat obehörig åtkomst till personuppgifter. Obehörig är den som inte har legitim anledning att ta del av en handling eller uppgift i sin tjänsteutövning. Bestämmelser om sekretess utgör ofta men inte alltid en utgångspunkt för vilka uppgifter som någon får ta del av. Genom en ändamålsenlig behörighetsstyrning kan det säkerställas att ingen obehörig åtkomst sker inom verksamheten. Behörighetsstyrning sker genom att bland annat bedriva ett arbete med att avgöra hur stor tillgång till uppgifter i ett verksamhetssystem som en medarbetare med en viss funktion eller roll ska ha. Det är viktigt att behörigheterna är anpassade och begränsade till det som är nödvändigt och i enlighet med gällande rättslig reglering. Dessutom behöver behörigheterna löpande kontrolleras och följas upp samt att åtkomstkontroller genomförs. En felaktig eller bristfällig behörighetsstyrning kan leda till exempelvis inskränkningar av den enskildes integritet eller personuppgiftsincidenter.

Den fördjupade kontrollen avser undersöka hur behörighetsstyrning används för att begränsa vilka uppgifter som medarbetarna får ta del av. Verksamhetens rutiner för tilldelning av behörigheter och åtkomster i IT-system kommer att granskas. Kontrollen kommer även omfatta verksamhetens uppföljning av medarbetares behörigheter och åtkomst till personuppgifter i IT-system samt om logg-/åtkomstkontroller används för att upptäcka och motverka obehörig åtkomst.

Syftet med den fördjupade kontrollen är att undersöka om medarbetares tillgång till personuppgifter är anpassade och begränsade till det som är nödvändigt för att medarbetaren ska kunna utföra sina arbetsuppgifter, att åtkomstkontroller genomförs och att därmed risken för obehörig åtkomst inom verksamheten minimeras.

Tillvägagångssätt

Den fördjupade kontrollen kommer att genomföras i två delar. I del ett ombeds ni att besvara ett antal frågor samt att skicka in dokumenterade rutiner, styrande dokument eller liknande underlag avseende tilldelning av behörigheter och åtkomst till IT-systemet TendSIgn. I del två kommer uppföljande frågor att ställas.

Dataskyddsombudet kommer sedan att sammanställa underlaget i en delårsrapport som lämnas till er i maj/juni.

Obs! Det är mycket viktigt att frågorna besvaras av eller i samråd med rätt befattningar inom förvaltningen/bolaget för att resultatet ska bli korrekt. Säkerställ även en lämplig förankring av svaren inom organisationen innan de översänds till dataskyddsombudet.

Fördjupad kontroll 2022

Kontrollpunkt 11: Behörighetsstyrning (del 1)

Del 1: Ni ombeds besvara frågorna nedan samt skicka in dokumenterade rutiner, styrande dokument eller liknande underlag avseende tilldelning av behörigheter och åtkomst till IT-systemet TendSign.

- Beskriv systemets behörighetsstruktur och olika roller i systemet.
- Vilka roller får vilka behörigheter och vad baseras den bedömningen på?
- Vem beslutar om vilka som ska ha vilken behörighet?
- Hur ofta följs behörigheterna upp för att kontrollera att dessa är korrekta och anpassade efter medarbetarens arbetsuppgifter? Vem/vilka ansvarar för det?
- Beskriv hur åtkomstkontroller/kontroll av loggar kan genomföras i systemet.
- När och hur ofta genomförs åtkomstkontroller/kontroll av loggar?
- Vem/vilka ansvarar för åtkomstkontrollerna/kontroll av loggar?
- Finns det annan lagstiftning eller andra bestämmelser, utöver dataskyddsförordningen, som er verksamhet behöver beakta i arbetet med behörighetstilldelning? I så fall, vilken/vilka?
- Vilka andra åtgärder vidtas för att förhindra obehörig åtkomst till personuppgifter i systemet?
- Har verksamheten identifierat några personuppgiftsincidenter kopplat till felaktiga behörigheter?

Obs! Det är mycket viktigt att frågorna besvaras av eller i samråd med rätt befattningar inom förvaltningen/bolaget för att resultatet ska bli korrekt. Säkerställ även en lämplig förankring av svaren inom organisationen innan de översänds till dataskyddsombudet.

Underlaget ska ha inkommit till dataskyddsombudet **senast den 10 mars 2022.**

Har du frågor, kontakta ditt huvudansvarige dataskyddsombud.

Fördjupad kontroll 2022

Kontrollpunkt 11: Behörighetsstyrning (del 2)

Del 2: Utifrån vad som framkommit i del 1 av den fördjupade kontrollen ombeds ni besvara frågorna nedan.

1. Hur många personer har behörighet i systemet (inom aktuella enheter, men inklusive personuppgiftsbiträde, administratörer)?
2. Finns det instruktioner till personuppgiftsbiträdet? Om ja, översänd dessa. Om nej, varför inte?
3. Har ni konsekvensbedömt behandlingarna i systemet? Varför/varför inte?
   Har ni identifierat specifika risker kopplat till den nuvarande hanteringen av behörigheter? Varför/varför inte? Beakta såväl risker som uppkommer inifrån den egna organisationen som utanför (exempelvis intrång) för de registrerades rättigheter.
4. Planerar ni att ta fram rutiner för åtkomstkontroller/kontroll av loggar?

Obs! Det är mycket viktigt att frågorna besvaras av eller i samråd med rätt befattningar inom förvaltningen/bolaget för att resultatet ska bli korrekt. Säkerställ även en lämplig förankring av svaren inom organisationen innan de översänds till dataskyddsombudet.

Underlaget ska ha inkommit till dataskyddsombudet **senast 8 juni 2022**.

Dataskyddsombudet kan komma att ställa kompletterande frågor i samband med sammanställande av rapporten och/eller begära visning av systemet. Frågor kan komma att ställas såväl muntligen som skriftligen.

Har du frågor, kontakta ditt huvudansvarige dataskyddsombud.